GROUPS OF RATIONAL TRANSFORMATIONS IN A GENERAL FIELD*

BY

LEWIS IRVING NEIKIRK

Introduction.

Groups of linear transformations of a single variable of both finite and infinite orders are well known, but the only known examples of non-linear rational transformation groups in one variable are those given by the following writers: HERMITE, BETTI, and others have investigated special quantics, known as substitution quantics, with coefficients taken with respect to a prime modulus (p), which define substitutions on a set of residues (mod p) and generate finite groups (mod p). Substitution quantics with coefficients in a Galois field have been investigated by DICKSON in his dissertation,† where the reader will find a complete bibliography of the subject.

The object of this paper is to find all *non-linear* groups of rational transformations of a single variable. It is proved in § 1 that these groups of transformations define substitution groups on the roots of an equation $f(x) = 0$. They are a two-fold generalization of substitution quantics and form finite groups (mod $f(x)$). Section 2 is devoted to finding these transformations and section 3 to the conditions for the existence of such transformations in a general field F. The other articles apply and extend these results.

§1. *General developments.*

Consider a group G of rational integral transformations

$$T_i \equiv [x : \phi_i(x)],$$

$$\phi_i(x) = \sum_{j=0}^{j=m_i} \alpha_{ij} x^{m_i - j} \qquad (\alpha_{i0} \neq 0),$$

where the coefficients α_{ij} are elements of a general field F and the quantity x belongs to a set X_i in a field F' containing F. It is assumed that at least one m_i exceeds unity, so that the group is not linear.

* Presented to the Society (Chicago), April and December, 1909.

† L. E. DICKSON, *The analytical representation of substitutions on a power of a prime number of letters, etc.*, Annals of Mathematics, ser. 1., vol. 11 (1896), pp. 65–120, 161–183.

Let $T_i(X_i) = X'_i$. Then *

$$(a) \qquad X_i \equiv X'_i, \text{ for every } i.$$

$$(b) \qquad X_i \equiv X_{i'} \equiv X, \text{ for every } i \text{ and } i'.$$

(*a*) Since T_i^2 is in G, X'_i is a subset of X_i, and since T_i^{-2} is in G, X_i is a subset of X'_i. Therefore $X_i \equiv X'_i$.

(*b*) X_i must be a subset of $X_{i'}$ since $T_{i'}T_i$ is in G, and $X_{i'}$ must be a subset of X_i since $T_iT_{i'}$ is in G. Therefore $X_i \equiv X_{i'} \equiv X$.

Since T_i, of degree $m_i > 1$, has an inverse in G, let $T_i^{-1} = T_{i'}$. Then

$$T_iT_{i'} \equiv [x : x] = [x : \phi_i\{\phi_{i'}(x)\}],$$

whence

$$(1) \qquad \phi_i\{\phi_{i'}(x)\} = x,$$

so that x satisfies an equation of degree $m_im_{i'} > 1$, the leading coefficient being $\alpha_{i0}\alpha_{i'0} \neq 0$.

Therefore the elements of the set X are roots of an equation rational in F.

Let $X = (x_1, x_2, x_3, \cdots, x_n)$ be a set whose elements are the roots of an equation,

$$f(x) = \sum_{r=0}^{r=n} a_r x^{n-r} = 0,$$

with the coefficients in F and having no double root.

All the transformations reduce (mod $f(x)$) to degree $n-1$ or less.†

Let T_i change X according to the scheme

$$\begin{pmatrix} x_1 x_2 \cdots x_n \\ x_{i_1} x_{i_2} \cdots x_{i_n} \end{pmatrix}.$$

If any root is repeated in the lower line, T_i will not have an inverse in the group G. Therefore the lower line is a permutation of the upper line and T_i defines a substitution on the roots of $f(x) = 0$. Hence we have proved

THEOREM I. *The only non-linear groups of rational integral transformations on one variable are finite groups taken modulo $f(x)$ which define substitution groups on the roots of the equation $f(x) = 0$.*‡

§ 2. *Determination of the transformation corresponding to a given substitution.* §

Given a substitution on the roots of $f(x) = 0$,

$$S_i = \begin{pmatrix} x_1 x_2 \cdots x_n \\ x_{i_1} x_{i_2} \cdots x_{i_n} \end{pmatrix},$$

* BURNSIDE (*Theory of Groups*, p. 12) makes use of property (*a*) without explicit mention in the proof that if A_{-1} is the inverse of A, then A is the inverse of A_{-1}.

† H. WEBER, *Lehrbuch der Algebra*, vol. I, p. 170.

‡ The actual existence of these groups will be established in the next two articles.

§ L. E. DICKSON, Dissertation, l. c.

we seek the corresponding transformation T_i. We have the n linear equations

$$x_{i_t} = \phi_i(x_t) = \sum_{j=0}^{j=n-1} \alpha_{ij} x_t^{n-1-j} \qquad (t = 1, 2, \cdots, n)$$

between the n coefficients α_{ij}. From these

$$(2) \qquad \alpha_{ij} = \frac{\begin{vmatrix} x_1^{n-1} & x_1^{n-2} & \cdots & x_{i_1} & x_1^{n-j-2} & \cdots & 1 \\ x_2^{n-1} & x_2^{n-2} & \cdots & x_{i_2} & x_2^{n-j-2} & \cdots & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_n^{n-1} & x_n^{n-2} & \cdots & x_{i_n} & x_n^{n-j-2} & \cdots & 1 \end{vmatrix}}{\pm\sqrt{\Delta}} \qquad (j = 0, 1, 2, 3, \cdots, n-1)$$

where Δ is the discriminant of $f(x)$, so that

$$\pm\sqrt{\Delta} = \begin{vmatrix} x_1^{n-1} & x_1^{n-2} & \cdots & 1 \\ x_2^{n-1} & x_2^{n-2} & \cdots & 1 \\ \cdot & \cdot & \cdot & \cdot \\ x_n^{n-1} & x_n^{n-2} & \cdots & 1 \end{vmatrix} \neq 0.$$

We can also determine T_i by the Lagrangian interpolation formula

$$\phi_i(x) = \sum_{t=1}^{t=n} \frac{x_{i_t} f(x)}{(x - x_t) f'(x_t)}, \qquad f(x) = (x - x_1)(x - x_2) \cdots (x - x_n).$$

The coefficients of ϕ_i determined by either of these two methods are not necessarily contained in the general field F.

§ 3. *Condition for transformations with coefficients in F.*

THEOREM II. *The necessary and sufficient condition for the existence of the transformation T with coefficients in the field F on the roots of the equation $f(x) = 0$ with coefficients in F is that the substitution S be permutable with every substitution of the Galois group of $f(x) = 0$ for F.*

Let

$$S = \begin{pmatrix} x_t \\ x_{tS} \end{pmatrix} \qquad (t = 1, 2, \cdots, n).$$

Determine $\phi(x)$ by means of one of the two methods given in section 2. We have the equations

$$(3) \qquad x_{tS} = \phi(x_t) \qquad (t = 1, 2, 3, \cdots, n).$$

(1) Proof that condition is necessary. The coefficients of ϕ are in F by hypothesis. Hence we may apply to (3) the substitutions R of the Galoisian group.* Hence

$$x_{tSR} = \phi(x_{tR}).$$

But, by (3),

$$x_{tRS} = \phi(x_{tR}).$$

Hence $x_{tRS} = x_{tSR}$ for every t, and thus $RS = SR$.

(2) Proof that the condition is sufficient. By hypothesis, $RS = SR$ for every R in the Galoisian group.

Let $x_{tR} = x_p$. Then $x_{tSR} = x_{tRS} = x_{pS}$. Hence if R replaces x_t by x_p it replaces x_{tS} by x_{pS}. In § 2, $x_{1S}, \cdots, x_{nS}$ were denoted by $x_{i_1}, \cdots, x_{i_n}$. Hence if R replaces x_t by x_p, it replaces x_{i_t} by x_{i_p}. Hence the coefficients of ϕ given by equation (2) are unaltered by R and thus belong to F.

§ 4. *The representation of substitutions.*

The substitution

$$S_i \equiv \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_{i_1} & x_{i_2} & \cdots & x_{i_n} \end{pmatrix}$$

can be represented by the transformation

$$T_i \equiv [x_t : x_{\phi_i(t)}],$$

where

$$\phi_i(t) = \sum_{j=0}^{j=n} \frac{i_j f(t)}{(t-j) f'(j)}, \qquad f(t) = (t-1)(t-2)\cdots(t-n).$$

We may also determine the coefficients of

$$\phi_i(t) = \sum_{j=0}^{j=n-1} \alpha_{ij} t^{n-1-j}$$

from the n linear equations

$$\phi_i(t) = i_t \qquad (t = 1, 2, 3, \cdots, n).$$

The results are

$$\alpha_{ij} = \frac{\begin{vmatrix} 1^{n-1} & 1^{n-2} & \cdots & i_1 & 1^{n-2-j} & \cdots & 1 & 1 \\ 2^{n-1} & 2^{n-2} & \cdots & i_2 & 2^{n-2-j} & \cdots & 2 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ n^{n-1} & n^{n-2} & \cdots & i_n & n^{n-2-j} & \cdots & n & 1 \end{vmatrix}}{\pm\sqrt{\Delta}} \qquad (j = 0, 1, 2, 3, \cdots, n-1),$$

* The theorems used here are known as properties A and B of the Galois group. See DICKSON, *Introduction to the theory of algebraic equations*, p. 53.

where

$$\pm\sqrt{\Delta} = \begin{vmatrix} 1^{n-1} & 1^{n-2} & \cdots & 1 & 1 \\ 2^{n-1} & 2^{n-2} & \cdots & 2 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ n^{n-1} & n^{n-2} & \cdots & n & 1 \end{vmatrix} = \prod_{r=1}^{r=n-1} (n-r)!.$$

§ 5. *Special examples.*

1. Let $n = 3$ and

$$S_1 = (x_1 x_2 x_3), \qquad S_2 = (x_1 x_2).$$

Then

$$f(t) = t^3 - 6t^2 + 11t - 6, \qquad \phi_1(t) = -\tfrac{3}{2}t^2 + \tfrac{11}{2}t - 2,$$

$$\phi_2(t) = \tfrac{3}{2}t^2 - \tfrac{11}{2}t + 6.$$

These define the symmetric group on three letters.

2. Let $n = 4$ and

$$S_1 = (x_1 x_2 x_3 x_4), \qquad S_2 = (x_1 x_2)(x_3 x_4), \qquad S_3 = (x_1 x_2 x_3).$$

Then

$$f(t) = t^4 - 10t^3 + 35t^2 - 50t + 24, \qquad \phi_1(t) = -\tfrac{2}{3}t^3 + 4t^2 - \tfrac{19}{3}t + 5,$$

$$\phi_2(t) = -\tfrac{4}{3}t^3 + 10t^2 - \tfrac{65}{3}t + 15, \qquad \phi_3(t) = \tfrac{4}{3}t^3 - \tfrac{19}{2}t^2 + \tfrac{121}{6}t - 10.$$

These define the symmetric group on four letters.

§ 6. *Rational fractional transformations.*

The results of the previous articles can be extended to rational fractional transformations.

Consider a group G of transformations

$$T_i \equiv [x : \psi_i(x)],$$

where

$$\psi_i(x) = \frac{\phi_i(x)}{\theta_i(x)}, \qquad \phi_i(x) = \sum_{j=0}^{j=m_i} \alpha_{ij} x^{m_i - j}, \qquad \theta_i(x) = \sum_{j=0}^{j=n_i} \beta_{ij} x^{n_i - j}.$$

$\alpha_{i0} \neq 0$, $\beta_{i0} \neq 0$, while $\phi_i(x)$ and $\theta_i(x)$ have no common factor and at least one of the degrees m_i, n_i exceeds unity.

The coefficients α_{ij} and β_{ij} are elements of a general field F and the quantity x belongs to a set X in a field F'. As before, these transformations are associative and have the closure property. If T_i and $T_{i'}$ are inverses

$$T_i T_{i'} \equiv [x : x] = [x : \psi_i\{\psi_{i'}(x)\}]$$

and we have

$$\psi_i\{\psi_{i'}(x)\} = x \qquad (m_i n_i > 1).$$

This is either (a) *an equation of condition*, $f(x)=0$, or (b) *an identity*.

(a) In this case the transformations reduce [mod $f(x)$] to the integral form considered in the first part of the paper.*

(b) In this case,

$$y=\frac{\phi_i(x)}{\theta_i(x)} \quad \text{gives} \quad x=\frac{\phi_{i'}(y)}{\theta_{i'}(y)},$$

therefore to each y there is only one x and therefore $\phi_i(x)$ and $\theta_i(x)$ are linear. Case (b) is therefore excluded.

§ 7. *Representation of products of substitutions.*

Consider any k substitutions R_j of order r_j ($j=1,2,\cdots,k$) on the n roots of $f(x)=0$.

Take the products of powers of these substitutions of the form †

$$S_i=R_1^{y_1^{(i)}}R_2^{y_2^{(i)}}\cdots R_k^{y_k^{(i)}}\equiv\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_{i_1} & x_{i_2} & \cdots & x_{i_n}\end{bmatrix}.$$

The number of these products is

$$r=\prod_{j=1}^{j=k} r_j$$

and i will have the range $1,2,\cdots,r$.

When the basic substitutions $R_j(j=1,2,\cdots,k)$ are given, S_i will be determined by the exponents $y_1^{(i)}, y_2^{(i)}, \cdots, y_k^{(i)}$.

It is possible to represent all these substitutions by the transformations

$$T_i\equiv[x:\phi(x;y_1^{(i)},y_2^{(i)},\cdots,y_k^{(i)})] \tag{4}$$

where ϕ is determined by the generalized Lagrangian interpolation formula

$$\phi(x;y_1,y_2,\cdots,y_k)=\sum_{l=1}^{l=n}\sum_{j=1}^{j=r}\frac{x_{j_l}f(x)}{(x-x_l)f'(x_l)}\prod_{p=1}^{p=k}\frac{\theta_p(y_p)}{(y_p-y_p^{(j)})\theta'_p(y_p^{(j)})}$$

and

$$f(x)=\prod_{t=1}^{t=n}(x-x_t), \qquad \theta_p(y_p)=\prod_{s=1}^{s=r}(y_p-y_p^{(s)}).$$

When any particular set of y's as $(y_1^{(i)},y_2^{(i)},\cdots,y_k^{(i)})$ are substituted in the above it reduces to the regular Lagrangian formula and gives the $\phi_i(x)$ used in first part of this paper and therefore T_i. The function ϕ is a rational integral

* H. WEBER, *Lehrbuch der Algebra*, vol. 1, p. 170.

† No two sets $(y_1^{(i)},y_2^{(i)},\cdots,y_k^{(i)})$ are alike but no assumption is made concerning the corresponding S_i.

function of x whose coefficients are rational integral functions of the k parameters $y_1, y_2, \cdots, y_k$. The numerical coefficients will be contained in the field F when S_i fulfills the conditions in Theorem II for every value of i.

Any set of substitutions S_i $(i = 1, 2, \cdots, r)$ where each substitution is characterized by a particular set of values $y_1^{(i)}, y_2^{(i)}, \cdots, y_k^{(i)}$ of the k parameters $y_1, y_2, \cdots, y_k$ can be represented by transformations T_i determined as above. *It is therefore possible to represent* an entire group of transformations by a single formula* (4).

UNIVERSITY OF ILLINOIS, URBANA, ILLINOIS.

* Some of the transformations may be repeated.